REMARKS

Claims 15-21, 23-24, 27-34, and 36-37 are pending in the present application, claims 22 and 35 having been cancelled without prejudice or disclaimer herein and claims 36-37 having been added. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

Claim 34 was objected to because of the abbreviation "DPA" in the claim. This has been corrected. Withdrawal of the objection is respectfully requested.

Claims 15-19, 22-24, and 27-34 were rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite. Applicant has amended the claims to address the Examiner's concerns, and overcome this rejection. With respect to claim 34, the language has been deleted and now appears in new claim 36. Applicant has recited "said each operation" to clarify which operation is being referenced. With respect to claims 27 and 28, Applicant has clarified that it is the step of storing the second set of instructions, and has deleted the word "respective". Claim 29 has been amended to refer to "the second set of instructions". Claim 32 has been amended in accordance with the Examiner's suggestions. Applicant respectfully submits that the claims are now fully in compliance with 35 U.S.C. §112. Withdrawal thereof is respectfully requested.

Claims 15-19, 22-24, and 27-34 were rejected under 35 U.S.C. §103(a) as unpatentable over Applicant's admitted prior art in view of Chow (U.S. Patent No. 6,594,761) and Kocher (U.S. Patent No. 6,278,783). Applicant previously indicated that a declaration under 37 C.F.R. §1.131 would be filed. Instead, however,

Applicant presents the following arguments as to why this rejection should be withdrawn on the merits.

Applicant has amended the claims such that claim 34 amended so as to cover only one embodiment of the implementation of the invention, whereas new claim 37 covers another embodiment of the implementation.

Claim 34 relates to an embodiment in which there is random selection of either the whole set of instructions for a first chain of operations in a normal state or this whole set of instructions in a complemented state (see lines 7-12 of page 4 of the specification). This embodiment is detailed in figure 1 and from line18 of page 5 to line 18 of page 6 and from line 1 of page 8.

The embodiment covered by claim 36 is the case detailed in figure 2 and from line 19 of page 6 to the end of page 7 and from line 1 of page 8. In this case, there is a random selection for each operation of the chain of operations; either this “each” operation is selected or the respective one which is complemented in the second chain of operations.

An additional claim 37 depends on claim 36 and recites that there is further a selection for using the message as it is or in complemented state.

Applicant respectfully submits that both these embodiments are clearly explained in the application and that both claims 34 and 36 distinguish the invention of the cited prior art. In the last Office Action, the Examiner rejected claim 34 for obviousness over the admitted prior art in view of the teachings of Chow and Kocher. The admitted prior art is the statement from the bottom of page 1 to page 2. According to this admitted prior art, there is identity between the chains executed in both entities. As to Chow, detailed explanations have already been given in the reply

to the preceding Office Action, which is incorporated by reference herein. Applicant submits the following additional remarks.

Chow deals with a user's ability to obtain and run unauthorized or unlicensed software (col. 1, lines 18-22) and with preventing attackers from making copies and making arbitrary changes (col. 2, lines 2-5). The method and system of the Chow invention recognizes that attackers cannot be prevented from making copies and making arbitrary changes (col. 3, lines 45-47). Figure 2 discloses a preferred embodiment of the invention, consisting of a three-part compiler (col. 6, lines 10-13), the middle part operating the invention for making the software tamper-resistant (col. 6, lines 29-32). At the output of the compiler, the generated tamper-resistant object code is available to the user to link and load (col. 6, lines 36-39).

Chow states, from line 50 of column 18 to line 13 of column 19, that there can be complementation of some Boolean operations. However, there is no teaching to make any random selection: lines 65 and 66 only state that some operations may be performed in their normal state, whereas some other operations may be performed in their complemented state, and the example given in that connection deals with complementation (or not) of variables known in advance.

Beginning on line 28 of column 20, the case of DES (Data Encryption Standard) is considered by Chow. However, the explanations which are given in that connection mainly concern the DES keys (line 30 of column 20). It thus appears that Chow provides the person ordinarily skilled in the art with teachings as to how to provide an object code in a single finalized state such that third parties will be practically prevented from understanding how it works, so that these third parties will be prevented to alter this code so that it works in another manner. This is quite

different from the present claimed invention, where no copy of the software is available to the third parties, and which deals with steps to be taken during the execution of a software program so as to resist to Differential Power Attacks (DPA). Further, Chow fails to recognize that there may be any random selection when executing a software program in a microcircuit card, the result of which is to be compared to the result of another software program in a server entity.

Applicant respectfully submits that, since Chow deals with a technical problem completely different from the one considered by the invention, there would have been no reason why a person ordinarily skilled in the art would have been "obviously" led to think to combine this Chow teaching with the conventional authorization process between a server entity and a microcircuit card. Applicant submits that making such a connection can only be made after understanding the invention, i.e., after the invention was made.

Kocher has also been analyzed in Applicant's reply to the preceding Office Action, which is incorporated by reference herein. Applicant further notes that Kocher teaches a complicated way to introduce randomization (see the wording of claim 1) with splitting each message in two parts so as to produce four values (M1, M2, M1P, M2P) for each message.

Applicant respectfully submits that Kocher fails to realize any possible use in case of validation as in the invention, with any comparison of the results of two parallel chains of operations. Further, Kocher would have led the person ordinarily skilled in the art to proceed with a splitting of a message in two parts. Applicant submits that Kocher fails to teach the person ordinarily skilled in the art that a mere selection to complement or not the whole of a DES itself (see claim 34)

or to complement or not the successive operations of a DES (claim 36), which is quite simpler to what is proposed in Kocher, is sufficient for an appropriate protection.

For at least these reasons, Applicant respectfully submits that claims 34 and 36 are patentable over the cited prior art, alone or in combination as proposed in the Office Action. Claims 15-21, 23-24, and 27-33 are believed to be patentable in and of themselves, and for the reasons discussed above with respect to claims 34 and 36.

If the Examiner has any questions he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:srd
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\R\RINU\Akkar1\pto\2011-11-02Amendment.doc